Cyber War and Lessons from History in the Digital Age

Hughes, Robert G.; Shaffer, Ryan

Published in:
Intelligence and National Security

DOI:
10.1080/02684527.2018.1502002

Publication date:
2018

Citation for published version (APA):
Hughes, R. G., & Shaffer, R. (2018). Cyber War and Lessons from History in the Digital Age. *Intelligence and National Security*, 1-6. https://doi.org/10.1080/02684527.2018.1502002

Review essay

Cyber War and Lessons from History in the Digital Age

R. Gerald Hughes and Ryan Shaffer

Understanding Cyber Conflict: Fourteen Analogies, edited by George Perkovich and Ariel E. Levite, Washington DC, Georgetown University Press, 2017, xii+298 pp. $34.95 (paperback), ISBN: 9781626164987.

> '[C]ybersecurity is one of the greatest challenges we face as a nation.' President Barack Obama, The White House, Washington DC, 2 December 2016.[1]

> 'We must take into account the plans and directions of development of the armed forces of other countries … Our responses must be based on intellectual superiority, they will be asymmetric, and less expensive.' President Vladimir Putin, Annual Address to the Federal Assembly of the Russian Federation, 11 May 2006.[2]

Much used, although often little understood, the terms 'cyber warfare' and 'cyber conflict' litter the Internet and the print media in the guise of a variety of revelatory exposes, confessions, exclusives and alarmist headlines. In short, cyber conflict entails activities – at either the state or sub-state level – whereby attempts to damage an adversary through attacking computers, information networks or any other facet of the modern Information Technology (IT) society. *Understanding Cyber Conflict* represents an attempt to assess current debates and past and future developments. This anthology, edited by George Perkovich and Ariel E. Levite, examines how governments are struggling with the unprecedented role of cyber issues as countries face threats with thievery, subversion, terrorism, covert operations and warfare. With fourteen chapters by government officials and scholars from Israel, Switzerland, the United Kingdom and the United States, the book presents historical analogies to provide insight into the capabilities, risks and preventative abilities of cyber technology. George Perkovich and Ariel E. Levite's 'Introduction' explains how vital it is to understand the benefits and pitfalls of cyber technology by discussing historical cases of new technology shaping weaponry, war and preventing conflict. They argue, 'To realize its benefits, and to minimize the technology's destructive potential, the widest possible range of societies and states must learn to steward it wisely' (p. 13). Through historical analysis of earlier technologies, the authors shed light on military-technological issues surrounding the use of cyber weapons, how effective they could be in a war and preventing cyber conflict.

> Human beings think, learn, and communicate through analogies. We use analogies – naturally, often without trying– to familiarize that which is new. As Richard E. Neustadt and Ernest R. May recorded in their classic study, *Thinking in Time,*[3] policymakers and pundits regularly invoke analogies as they struggle to make sense of and affect new situations, often without adequate reflection. This practice occurs now regarding the cyber world, which is evolving with an ever-quickening pace (p. 1).

Understanding Cyber Conflict is divided in three sections with the first exploring cyber weapons, including capabilities for intelligence and striking purposes, which the authors compare with earlier technologies.[4] Michael Warner explores intelligence and counter-intelligence in cyberspace by detailing how computers are an extension of what humans have done for intelligence throughout history, but he argues with cyber operations the scale of exploitable targets is unprecedented with policy questions that did not exist with earlier technologies, like radio or telegraph. In 'Nonlethal Weapons and Cyber Capabilities', Robert E. Schmidle Jr., Michael Sulmeyer and Ben Buchanan look at nonlethal weapons and cyber capabilities which, they assert, 'may be useful to analogize' in 'four areas: their ability to incapacitate, the reduced collateral damage they inflict, the reversibility of their effects, and their ability to deter' (p. 31). They conclude their chapter by asserting that

> despite very real concerns about a coming conflict in cyberspace, some of the most promising features of cyber capabilities are also common with other nonlethal weapons: their effects need not be permanent and could possibly be so narrowly tailored that collateral damage is all but eliminated. As with any other instrument of military power, cyber capabilities should be used only as a last resort. But when military coercion is required to secure US interests, cyber capabilities–like nonlethal weapons–may offer US military commanders the opportunity to do so in ways that greatly reduce the incidence of death and destruction on all sides of a future conflict (p. 41).

Next in *Understanding Cyber Conflict*, 'Cyber Weapons and Precision-Guided Munitions' by James M. Acton compares cyber weapons and precision-guided munitions, such as cruise missiles, with attention to reducing collateral damage and decreasing distance from targets, which changed national decision-making about force and provokes questions about cyber weapons' limitations for achieving strategic political-military objectives. Likewise, in 'Cyber, Drones, and Secrecy', David E. Sanger discusses commonalities between armed drones and cyber weapons through an analysis about advantages and 'secret' decision-making, finding that government 'fear of revealing the size and scope of' American cyber capabilities 'has frozen many of the most important' public 'discussions' (p. 76). Regardless, Sanger notes that the utility of such means continues to raise important issues for policymakers.

> Today as President Trump has taken over…mature drone and cyber programs, clearly the two weapons raise similar moral and legal issues that future presidents will have to grapple with. Indeed, Pentagon officials openly wonder whether the next major global conflict might open in cyberspace and be prosecuted by a range of new, autonomous weapons–not only aerial unmanned vehicles but also undersea ones. And yet these drone and cyber weapons, nurtured by the same policymakers and sometimes used in the same conflicts, have taken very different paths–as have the questions surrounding their use… In short, the decisions President Donald Trump will have to make will likely be similar to the vexing choices Mr. Obama faced on whether to use cyber weapons as an alternative to more traditional forms of low-level warfare, even while recognizing that, sooner or later, that may escalate the global use of

> cyber weapons. Only at the end of the Obama administration was it possible to start comparing the issues, and lessons, raised by using drones and cyber weapons (pp. 63, 64).

The second section of *Understanding Cyber Conflict* centers on differing conceptions of cyber war through historical comparisons about transformations in modern warfare.[5] Here, the Russian case is instructive. In 2004, Vladimir Kvachkov, a former GRU officer, stated that: 'A new type of war has emerged, in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare - information warfare.'[6] In his chapter 'Cyber War and Information War à la Russe', Stephen Blank looks at recent Russian offensive cyber operations and information warfare against its neighbors Estonia, Georgia and Ukraine, and argues it is a continuation of Soviet Union strategy to create insecurity. Moscow's post-2014 interventions in Crimea and Eastern Ukraine were modeled on the actions against Estonia and Georgia (in 2007 and 2008 respectively).

> The greater duration and intensity of the Ukraine conflict reflects the deeper political-economic connections between Russia and Ukraine and the greater stakes Russia perceives in repelling Western influence over Ukraine's future. Russian leaders perceived the onset of the crisis–that is, the demonstrations against Viktor Yanukovych's government–and the subsequent departure of Yanukovych as a coup conducted with, at least, the collusion of the West.[7] As such, the situation provided stark confirmation of the Kremlin's portrayal of existential US-led hostility to Russian interests. As in Estonia, Russian actors mounted intense IO to shape how Ukrainians, Russians, and international audiences perceived the unfolding events. These operations were conducted through all media, especially Web-based outlets. Opinion surveys and anecdotal reporting in Russia indicate the effectiveness of these efforts in shaping perceptions in Russia (if not elsewhere) (p. 91).

If the subsequent Russian cyber attack on Ukraine was actually instigated (directly or indirectly) by Moscow then this suggests a continuation of the kind of strategic logic that was previously seen in the case of Georgia.

> [In Georgia] where capabilities to attack the energy infrastructure were put in place but not activated. In Georgia the Georgian state did not escalate the conflict, and Western powers did not intervene. Russian cyber operators did not then have cause to attack Georgia's energy supply system. Conversely, the attack on the energy supply to Russian-held Crimea was, in Russian eyes, an escalation that invited a somewhat symmetrical response. Ukraine's energy supply was cut off–the symmetrical part–but the method was a sophisticated cyber penetration and attack when compared to the simple toppling of transmission towers. Taken together, the Georgian and Ukrainian examples reflect [the] logic of deterrence and compellence by cyber means. A capability to do harm is emplaced to deter adversaries from acting against Russian interests. When the adversary is restrained, the cyber attack is not unleashed,

> but when the adversary attacks Russian interests, Russian actors inflict a roughly proportionate response (p. 92).

Meanwhile, the Russian government, naturally, denies accusations of engaging in cyber warfare against other states as a matter of course. (The Soviet Union did much the same with regard to its 'dirty tricks' before its dissolution in 1991). That said, an analysis by the US Defense Intelligence Agency (DIA) in January 2017 did identify key elements of Moscow's 'Information Confrontation' (*informatsionnoye protivoborstvo* (IPb)/ информационное противоборство).[8]

> Russia views the information sphere as a key domain for modern military conflict. Moscow perceives the information domain as strategically decisive and critically important to control its domestic populace and influence adversary states. Information warfare is a key means of achieving its ambitions of becoming a dominant player on the world stage.
>
> Since at least 2010, the Russian military has prioritized the development of forces and means for what it terms "information confrontation," which is a holistic concept for ensuring information superiority, during peacetime and wartime. This concept includes control of the information content as well as the technical means for disseminating that content. Cyber operations are part of Russia's attempts to control the information environment.[9]

The national security apparatus in Moscow divides its 'Information Confrontation' (IPb) techniques into two categories: a) 'Informational-Technical'; and b) 'Informational-Psychological'. The former 'is roughly analogous to computer network operations, including computer-network defense, attack, and exploitation.' The latter term relates to 'attempts to change people's behavior or beliefs in favor of Russian governmental objectives.'[10] In 2011, the Russian government directed its cyberwar capabilities towards the Arab Spring and the emerging civil war in Syria.[11] In 2017, the US DIA report concluded that President Vladimir Putin had personally directed a Russian campaign, with cyber attacks and the dissemination of false information very much to the fore, so as to assist Donald Trump in the presidential campaign against Hilary Rodham Clinton in 2016. Putin repeatedly denied accusations of interference but conceded that 'patriotically minded' Russian hackers may have done so. (This, of course, echoes Moscow's claim that any Russian citizens fighting in eastern Ukraine are 'volunteers'. Even said, Putin's statement was a shift from outright denial and he asserted that hackers 'are like artists', essentially free spirits whose inclinations and motives shift with time, opportunity and mood. 'If they are patriotically minded, they start making their contributions–which are right, from their point of view–to fight against those who say bad things about Russia' but 'we're not doing this on the state level'.[12]

Next, in 'An Ounce of (Virtual) Prevention?', John Arquilla delves deeper into the historical record, analyzing preventative force from the Napoleonic Wars until the Second World War and compares it to using cyber capabilities to slow Iran's uranium enrichment abilities, but argues such preventive actions provoke 'defensive measures' and 'a persistent fear of preventive attack may spark very aggressive action' (pp. 107-8). In contrast, Francis J. Gavin examines how

railroad technology was an 'element' of the crisis that led to First World War with the ambiguities of military mobilization for offensive and defensive purposes, and finds similarities and differences in how cyber shortened space and time for leaders to make decisions. During foreign policy crises, Gavin notes that the most popular historical analogy invoked amongst US policymakers and commentators is Appeasement and the Munich Agreement.[13] He asserts that scholars of international relations, by contrast, are more likely to refer to July crisis of 1914 (p. 111). Also studying the First World War, Nicholas A. Lambert reviews the significance of Britain using its global reach with telegraph and undersea cables in economic warfare and how it has parallels with a cyber-attack, but 'the British experience' shows 'that the infrastructure of a globalized economic system makes for a weapon of mass destruction rather than a precision strike weapon' (p. 143). Whereas with Pearl Harbor, Emily O. Goldman and Michael Warner explain how it was more of an American intelligence analysis failure about Japan rather than a 'surprise,' and they conclude that countries like the United States with militaries and economies that depend on the Internet must work harder at 'cyber Pearl Harbor' prevention and responses.

In the third and final section of *Understanding Cyber Conflict*, the authors discuss preventing and managing cyber conflict through historical experiences that involved evolving technology playing important roles in war.[14] Steven E. Miller compares nuclear technology with cyber technology by highlighting trajectories of dual-use technologies and finds cyber is 'very different' in 'a number of fundamental respects,' including deterrence, arms control and nonproliferation that does not transfer well to the cyber framework (p. 161). In another chapter that discusses Pearl Harbor (itself the subject of many historical analogies),[15] John Arquilla analyzes how Americans failed to learn lessons shortly after Pearl Harbor about defending from sea attacks and compares the situation to an 'inadequate' government and private industry response to protecting computers, networks and data. Turning to ethical and legal concerns, Dorothy E. Denning and Bradley J. Strawser apply air defense principles to historical cyberspace examples showing 'that, when properly understood and executed, is neither offensive nor necessarily harmful and dangerous' (p. 207). Whereas, Peter Feaver and Kenneth Geers draw from President Dwight D. Eisenhower's pre-delegation policy of allowing military commanders to use nuclear weapons in specific situations, which is compared to changes in how quickly leaders must 'manage' transformations brought by cyberspace. Lastly, Florian Egloff describes reducing cyber threats with an assessment of historical lessons from naval privateering when governments hired private actors for countering attacks, and argues the analogy 'allows for a rich understanding of the forces giving rise to the multiplicity of actors shaping the institution of privateering and eventually leading to its abolishment' (p. 242).

Understanding Cyber Conflict makes a solid contribution to an important, but sometimes neglected part of national security by offering possibilities and versatilities of cyber capabilities and conflict through analogies. George Perkovich and Ariel E. Levite's conclusion explores the challenges that countries and the international community faces with cyber conflict, writing 'there is a tension between one's potential interest in using cyber operations to exercise control over one's population or to weaken or otherwise harm adversaries, and one's interest in preserving the functionality of the global cyber system' (p. 268). In addition to summarizing characteristics of cyber weapons and differences with military technologies, they also broadly describe private and government policies and activities that could prevent and manage cyber

conflict as well as issues that moderate offensive cyber activities that effect countries in different ways. With chapters written by authors ranging from National Security Agency and US Cyber Command officials to journalists and scholars, the historical examples and analyses shed light on both the unpredictable impact fast-paced and evolving technology has on conflict and what lessons can be learned from technology's role in war. Some historians will be critical of the methodology that uses historical examples to understand contemporary situations with differing technologies, often radically so, although the editors do note that the differences in the comparisons 'are as important to understand as [are the] similarities' (p. 2). For instance, scholars of British history will quibble with some of the generalisations about the British Empire during the First World War as the causes of war and consequences of war have multitude of factors that were not fully addressed in any of the chapters. In any case, the notion that statesmen learn from history is almost always dismissed as a chimera by historians. When refuting this Hegel is nearly always invoked ('Rulers, Statesmen, Nations, are wont to be emphatically commended to the teaching which experience offers in history. But what experience and history teach is this – that peoples and governments never have learned anything from history, or acted on principles deduced from it.').[16] Yet, on balance, government officials and academics interested in the potential use, effectiveness and management of cyber conflict will nevertheless find this anthology a useful addition to the emerging and rapidly expanding literature.

References

- William Booth, 'Ukraine's parliament votes to oust president; former prime minister is freed from prison', *Washington Post*, 22 February 2014.
- Defence Intelligence Agency, *Russian Military Power: Building a Military to Support Great Power Aspirations* (Washington DC: Defence Intelligence Agency, 2017).
- Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College - NDC Fellowship Monograph Series, 2016).
- Georg W.F. Hegel, *The Philosophy of History* (New York: Dover 1956).
- R. Gerald Hughes, '"The Best and the Brightest": The Cuban Missile Crisis, the Kennedy administration, and the lessons of history' in Len Scott and R. Gerald Hughes (eds), *The Cuban Missile Crisis: A Critical Reappraisal* (New York: Taylor & Francis, 2016) 117-141.
- R. Gerald Hughes, *The Postwar Legacy of Appeasement: British Foreign Policy since 1945* (New York: Bloomsbury, 2014).
- R. Gerald Hughes, 'The Ghosts of Appeasement: Britain and the legacy of the Munich Agreement', *Journal of Contemporary History*, 48/4 (2013) 688-716.
- Clark Mindock (New York), 'Vladimir Putin hints 'patriotic' private Russian hackers could have meddled in 2016 US election', *The Independent* (London), 1 June 2017.
- Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Freedom Press, 1986).
- President Barack Obama, 'Statement by the President on the Report of the Commission on Enhancing National Cybersecurity', The White House, Washington DC, 2 December 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity (accessed 30 June 2018).

- Dominic Tierney, '"Pearl Harbor in Reverse": Moral Analogies in the Cuban Missile Crisis', *Journal of Cold War Studies*, 9/3 (2007) 49-77.

R. Gerald Hughes
Centre for Intelligence and International Security Studies
Aberystwyth University
E-mail: rbh@aber.ac.uk

Ryan Shaffer
Independent scholar
E-mail: ShafferRyan9@gmail.com
http://orcid.org/0000-0002-6766-2194

Notes

[1] President Barack Obama, 'Statement by the President on the Report of the Commission on Enhancing National Cybersecurity', The White House, Washington DC, 2 December 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity (accessed 30 March 2018).

[2] Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College - NDC Fellowship Monograph Series, 2016) 3.

[3] Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: Freedom Press, 1986).

[4] Section I. 'What Are Cyber Weapons Like?'; Chapter 1. Michael Warner, 'Intelligence in Cyber - and Cyber in Intelligence', 17-29; Chapter 2. Lt. Gen. Robert E. Schmidle Jr. (USMC, Ret.), Michael Sulmeyer, and Ben Buchanan, 'Nonlethal Weapons and Cyber Capabilities', 31-44; Chapter 3. James M. Acton, 'Cyber Weapons and Precision-Guided Munitions', 45-60; Chapter 4. David E. Sanger, 'Cyber, Drones, and Secrecy', 61-78.

[5] Section II. 'What Might Cyber Wars Be Like?'; Chapter 5. Stephen Blank, 'Cyber War and Information War à la Russe', 81-98; Chapter 6. John Arquilla, 'An Ounce of (Virtual) Prevention?', 99-110; Chapter 7. Francis J. Gavin, 'Crisis Instability and Preemption: The 1914 Railroad Analogy', 111-122; Nicholas A. Lambert, 'Brits-Krieg: The Strategy of Economic Warfare', 123-146; Emily O. Goldman and Michael Warner, 'Why a Digital Pearl Harbor Makes Sense…and Is Possible', 147-157.

[6] Kvachkov was an ex-GRU officer who developed a 'theory of special operations', which included information warfare. Giles, *Handbook of Russian Information Warfare*, 3.

[7] In February 2010, Viktor Yanukovych was elected president of Ukraine. Strongly pro-Russian, Yanukovych was ousted four years later as a result of the 'Ukrainian Revolution'. William Booth, 'Ukraine's parliament votes to oust president; former prime minister is freed from prison', *Washington Post*, 22 February 2014. Yanukovych is currently living in exile in Russia.

[8] Trans. 'Information Confrontation'. For the Russian state 'information confrontation' and 'information war' are broad and inclusive concepts. One author notes that the 'distinction between информационное противоборство, (*informatsionnoye protivoborstvo*), information confrontation, and информационная война (*informatsionnaya voyna*), information war, is the subject of detailed debate in official Russian sources', although the distinctions are, in reality, superficial. Giles, *Handbook of Russian Information Warfare*, 6(n.)

[9] Defence Intelligence Agency, *Russian Military Power: Building a Military to Support Great Power Aspirations* (Washington DC: Defence Intelligence Agency, 2017) 37-38.

[10] Defence Intelligence Agency, *Russian Military Power*, 38.

[11] Giles, *Handbook of Russian Information Warfare*, 41-4.

[12] Clark Mindock (New York), 'Vladimir Putin hints 'patriotic' private Russian hackers could have meddled in 2016 US election', *The Independent* (London), 1 June 2017.

[13] For relevant recent studies on this, see R. Gerald Hughes, '"The Best and the Brightest": The Cuban Missile Crisis, the Kennedy administration, and the lessons of history' in Len Scott and R. Gerald Hughes (eds), *The Cuban*

Missile Crisis: A Critical Reappraisal (New York: Taylor & Francis, 2016) 117-14; R. Gerald Hughes, *The Postwar Legacy of Appeasement: British Foreign Policy since 1945* (New York: Bloomsbury, 2014); and R. Gerald Hughes, The Ghosts of Appeasement: Britain and the legacy of the Munich Agreement', *Journal of Contemporary History*, 48/4 (2013) 688-716.

[14] Section III. 'What Are Preventing and Managing Cyber Conflict Like?'; Chapter 10. Steven E. Miller, 'Cyber Threats, Nuclear Analogies? Divergent Trajectories in Adapting to New Dual-Use Technologies', 161-179; 11. John Arquilla, 'From Pearl Harbor to the "Harbor Lights"', 181-192; 12. Dorothy E. Denning and Bradley J. Strawser, 'Active Cyber Defense: Applying Air Defense to the Cyber Domain', 193-209; 13. Peter Feaver and Kenneth Geers, '"When the Urgency of Time and Circumstances Clearly Does Not Permit . . .": Pre-delegation in Nuclear and Cyber Scenarios', 211-230. 14. Florian Egloff, 'Cybersecurity and the Age of Privateering', 231-247.

[15] On this see, for example, Dominic Tierney, '"Pearl Harbor in Reverse": Moral Analogies in the Cuban Missile Crisis', *Journal of Cold War Studies*, 9/3 (2007) 49-77.

[16] Georg W.F. Hegel, *The Philosophy of History* (New York: Dover 1956) 6.